



QUALYS SECURITY CONFERENCE 2020

Securing Cloud & Container Workloads

Badri Raghunathan

Director, Product Management, Qualys, Inc.

Security Challenges in the Cloud

Lack of visibility or control on cloud resources

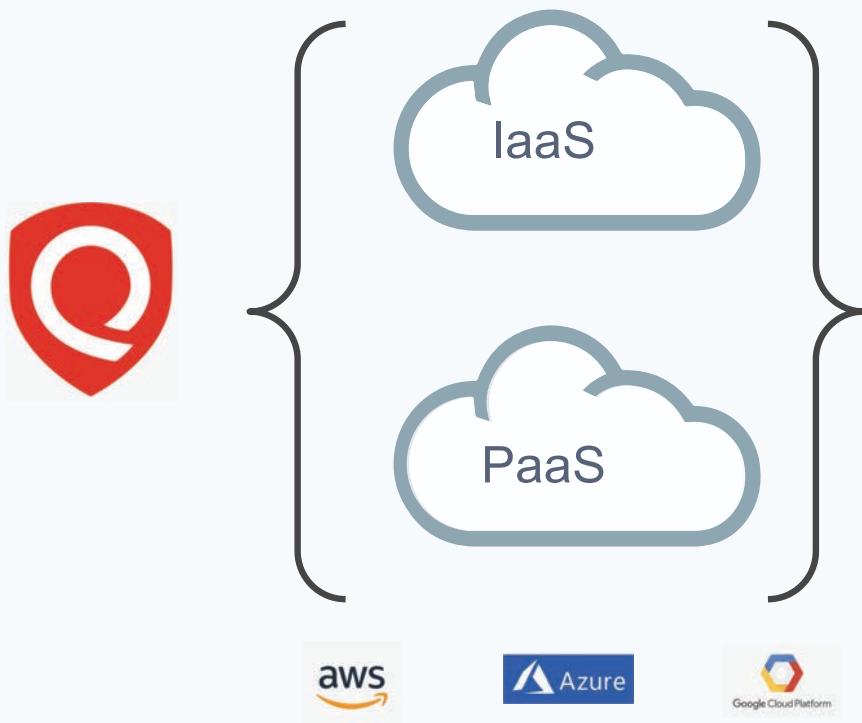
Misconfiguration of cloud services

Multi cloud environment magnifies security challenges

Lack of a unified security toolset/controls for on-prem & cloud workloads

Cloud Security

Cloud Workload Security with Qualys



Vulnerability Management

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management

Policy Compliance

- Policy Compliance (incl. Secure Configuration Assessment)
- File Integrity Monitoring

Application Security

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall
- API Security*

* Upcoming feature

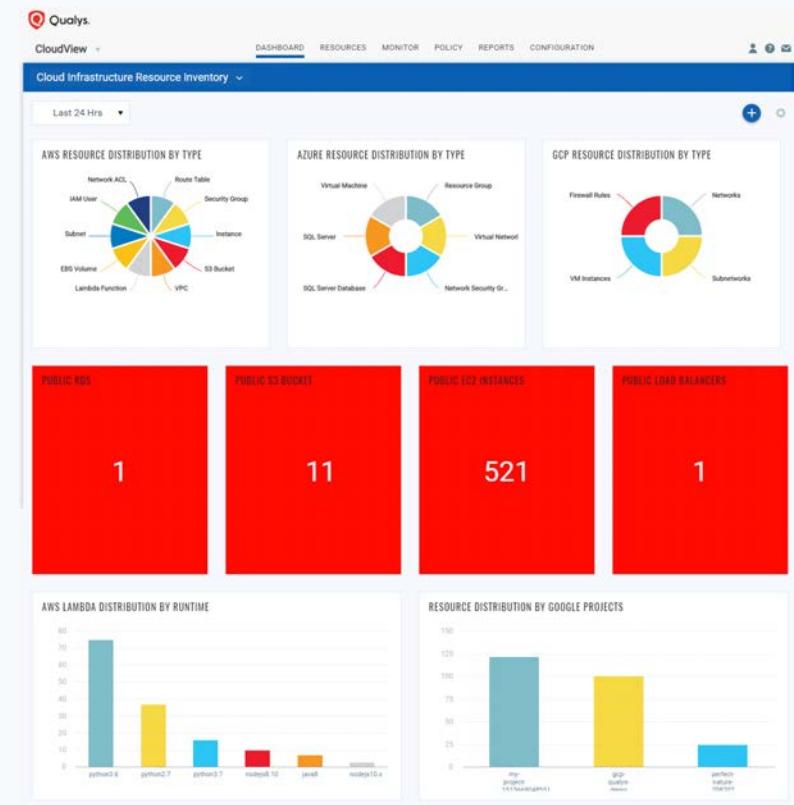
Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

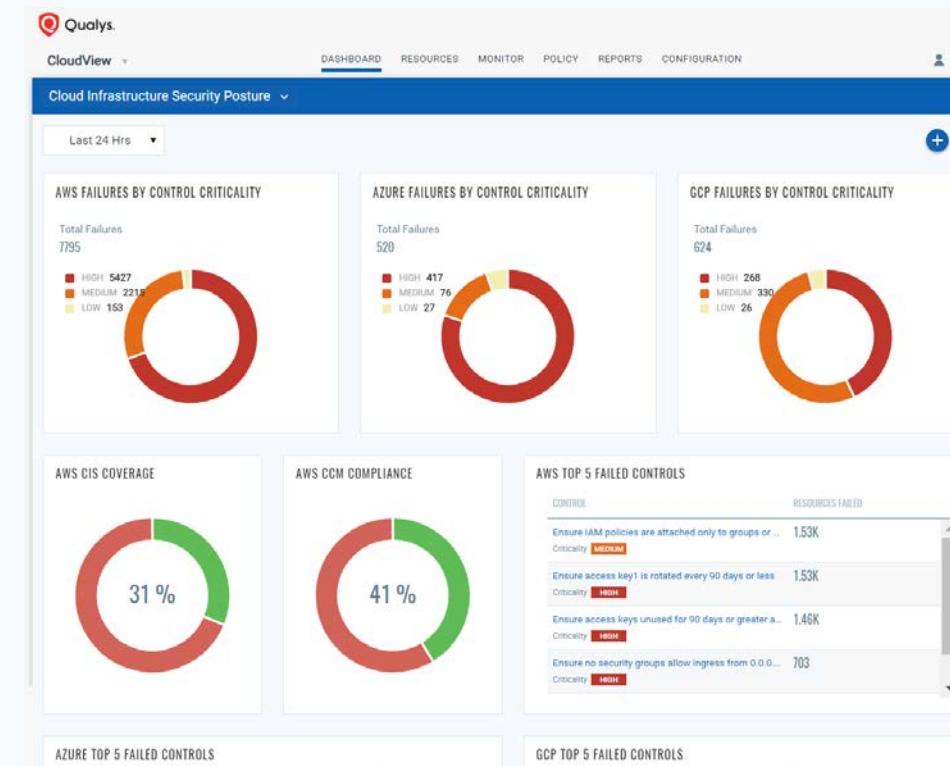


Compliance Assessment

Identify misconfigured resources

Detect resources that are non-compliant against standards such as CIS Benchmark

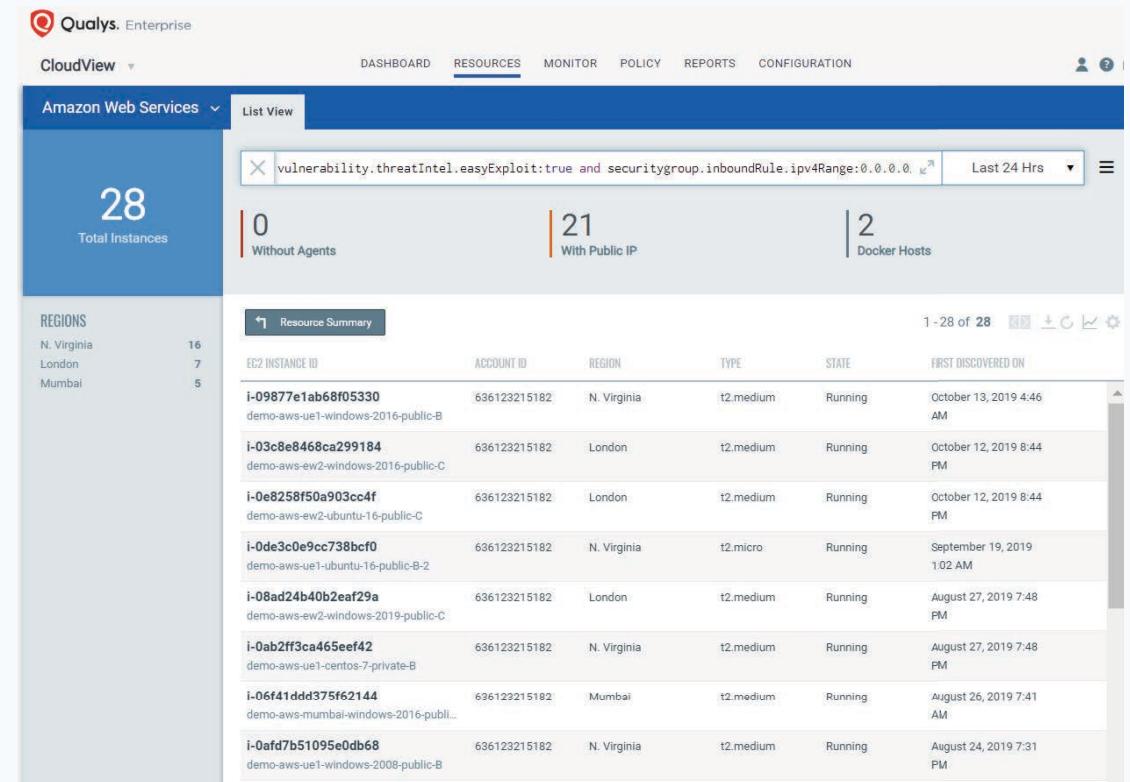
Identify top failed controls/account for prioritizing the remediation efforts



Correlate with Vulnerability Data

Identify vulnerable instances with public IP and associated with the misconfigured security groups

Use vulnerability information for cloud instances to prioritize threats better



Qualys. Enterprise

CloudView DASHBOARD RESOURCES MONITOR POLICY REPORTS CONFIGURATION

Amazon Web Services List View

28 Total Instances

0 Without Agents | 21 With Public IP | 2 Docker Hosts

vulnerability.threatIntel.easyExploit:true and securitygroup.inboundRule.ipv4Range:0.0.0.0/0 Last 24 Hrs

EC2 INSTANCE ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-09877e1ab68f05330	636123215182	N. Virginia	t2.medium	Running	October 13, 2019 4:46 AM
i-03c8e8468ca299184	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0e8258f50a903cc4f	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0de3c0e9cc738bcf0	636123215182	N. Virginia	t2.micro	Running	September 19, 2019 1:02 AM
i-08ad24b40b2eaf29a	636123215182	London	t2.medium	Running	August 27, 2019 7:48 PM
i-0ab2ff3caa465eef42	636123215182	N. Virginia	t2.medium	Running	August 27, 2019 7:48 PM
i-06f41ddd375f62144	636123215182	Mumbai	t2.medium	Running	August 26, 2019 7:41 AM
i-0afd7b51095e0db68	636123215182	N. Virginia	t2.medium	Running	August 24, 2019 7:31 PM

Serverless Visibility

NEW

Serverless Visibility –
Inventory support for
AWS Lambda functions

Best practices policy for
identifying
misconfigurations

The screenshot displays two Qualys CloudView dashboards for AWS Lambda functions.

Left Dashboard (Inventory):

- Header:** Qualys Express, CloudView, DASHBOARD, RESOURCES (selected), MONITOR, POLICY, REPORTS, CONFIGURATION.
- Search Bar:** resource.type:"Lambda Function", Last 24 Hrs.
- Summary:** 21 Total Lambda Functions.
- Regions:**
 - N. Virginia: 10
 - Ohio: 7
 - Mumbai: 2
 - Ireland: 1
 - Oregon: 1
- Runtime:**
 - nodejs4.3: 5
 - python3.7: 4
 - java8: 3
 - nodejs8.10: 3
 - python2.7: 3
 - 3 more
- Tracing:**
 - PassThrough: 20
 - Active: 1

Right Dashboard (Policy Evaluations):

- Header:** Qualys, CloudView, DASHBOARD, RESOURCES, MONITOR (selected), POLICY, REPORTS, CONFIGURATION.
- Search Bar:** policy.name:"AWS Lambda Best Practices Policy".
- Summary:** 11 Total Controls Evaluated, 1.61K Total Evaluations, 948 Pass, 667 Fail, 497 High, 48 Medium.
- Table:** List of 102 policy controls evaluated for Lambda functions, showing results, account, control name, criticality, and service.

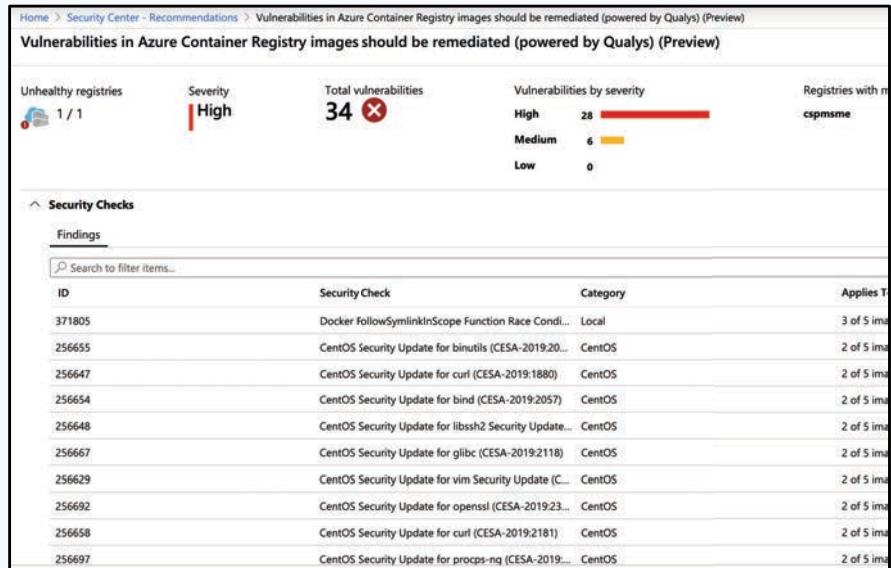
NEW

Built-in Security with Cloud Providers

Send findings into Azure, AWS, GCP Security Hubs

Access & investigate findings from within the Cloud Provider Security console

Native integration of vulnerability assessment of hosts, containers (MSFT Azure - Powered by Qualys)



Native Azure Host, Container Scanning (Powered by Qualys)

Container Security

Visibility into Container Infrastructure

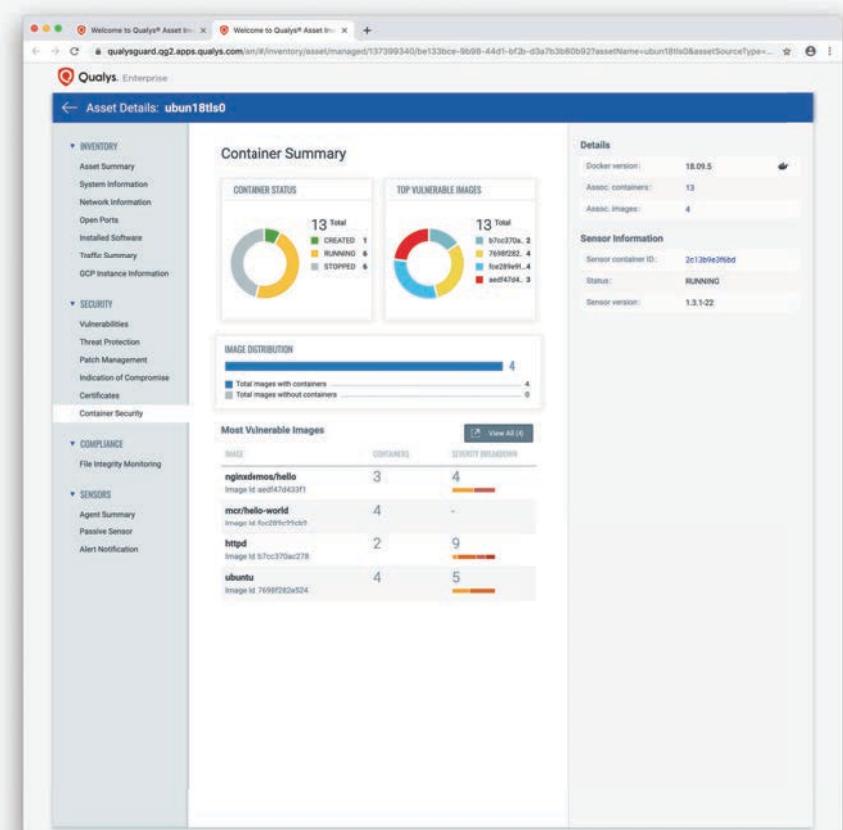
NEW

Inventory for all your container infrastructure (Included with VMDR)

Visibility into containers via Scanner, Cloud Agent, Container Sensor

Tracking DockerHub official images

Upgrade for security across DevOps pipeline



Correlating with Vulnerability Data

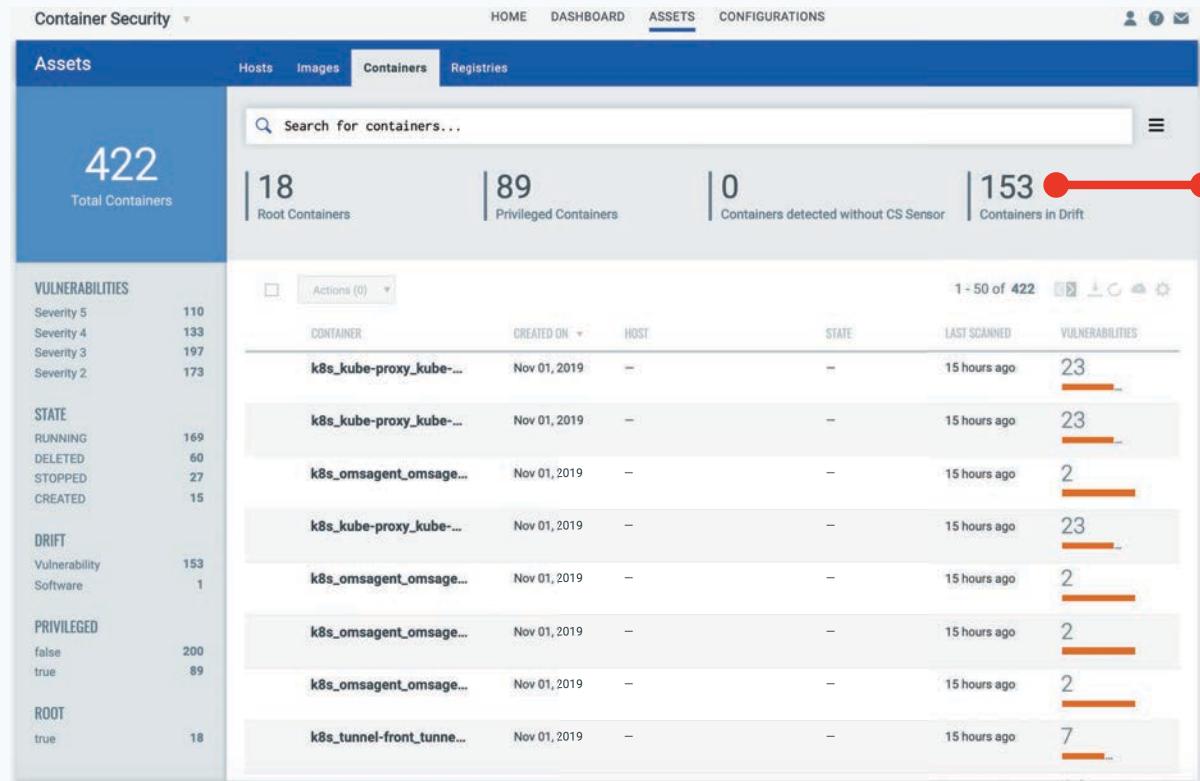
Search based on all attributes

The screenshot shows a Container Security interface. On the left, there's a sidebar with sections for Labels, Registry, and Vulnerabilities. The main area is titled 'Assets' and has tabs for 'Images' and 'Containers'. A search bar at the top contains the query: 'vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"'. Below the search bar is a table with columns: REGISTRY, REPOSITORY, CREATED ON, TAGS, CONTAINERS, and VULNERABILITIES. The table lists several Docker images, including 'elasticsearch', 'redis', 'kibana', 'node', 'httpd', 'cassandra', 'solr', 'tomcat', and 'kibana' again. Each row shows the image's creation date, tag, number of hosts it's running on, and a red progress bar representing its vulnerability score. A red box highlights the 'httpd' row, and a red arrow points from the 'Search based on all attributes' text to the search bar.

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch	Feb 06, 2018	latest	0	2
docker.io	redis	Feb 06, 2018	latest	1	3
docker.io	kibana	Feb 06, 2018	latest	0	3
docker.io	node	Feb 01, 2018	latest	0	3
docker.io	httpd	Jan 26, 2018	latest	1	3
docker.io	cassandra	Jan 23, 2018	latest	0	4
docker.io	solr	Jan 19, 2018	latest	0	14
docker.io	tomcat	Jan 18, 2018	latest	0	13
docker.io	kibana	Jan 17, 2018	latest	0	10

- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

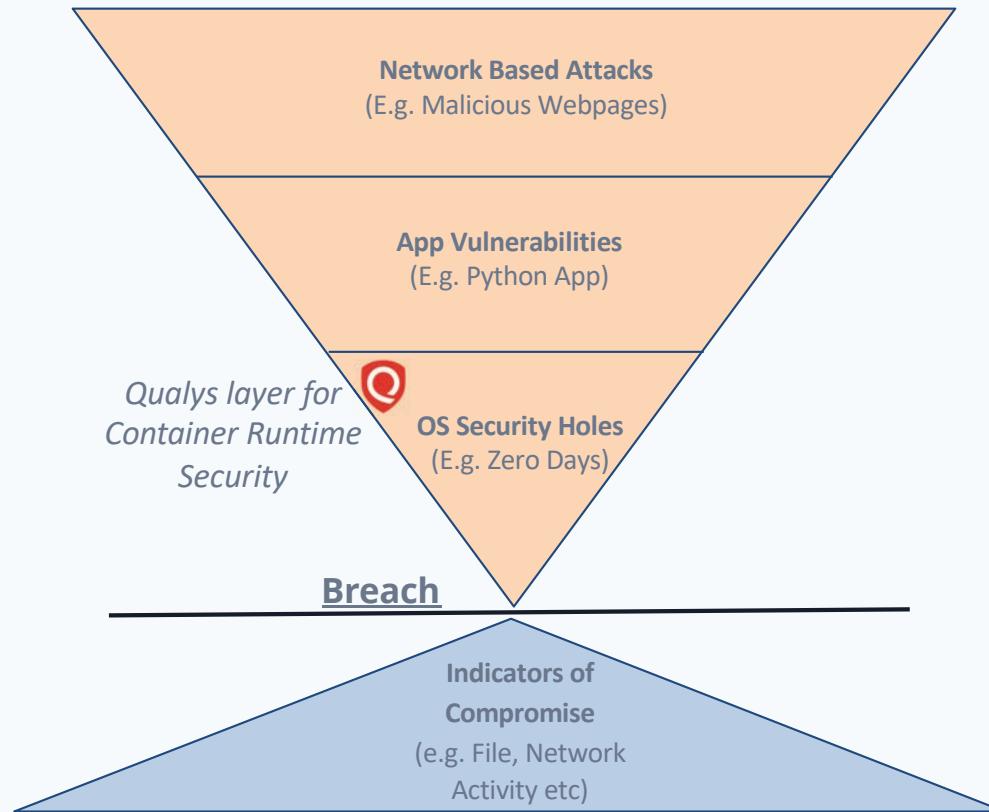
Detecting Runtime Drift



Identify potential breaches in containers

“Drift” Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc

Detection, Response for Containers



NEW

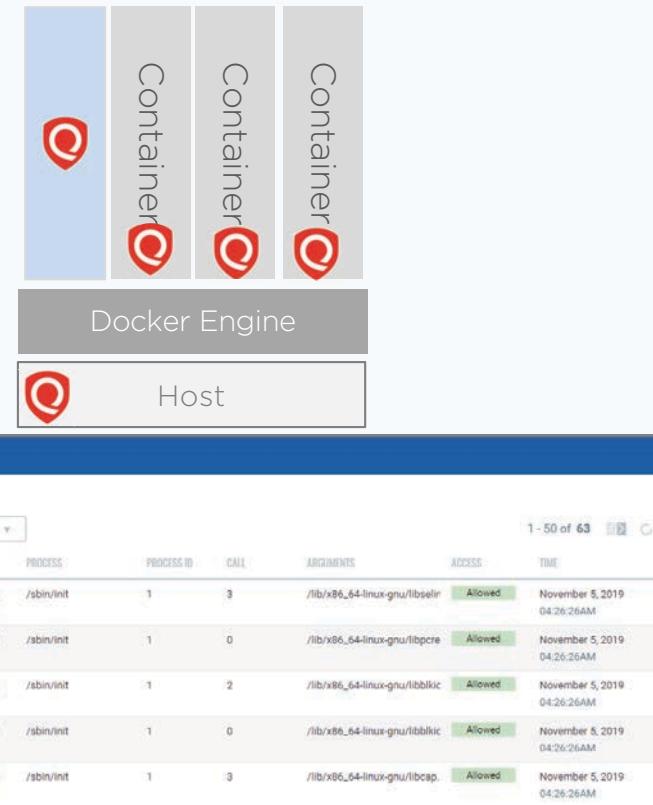
Container Runtime Security

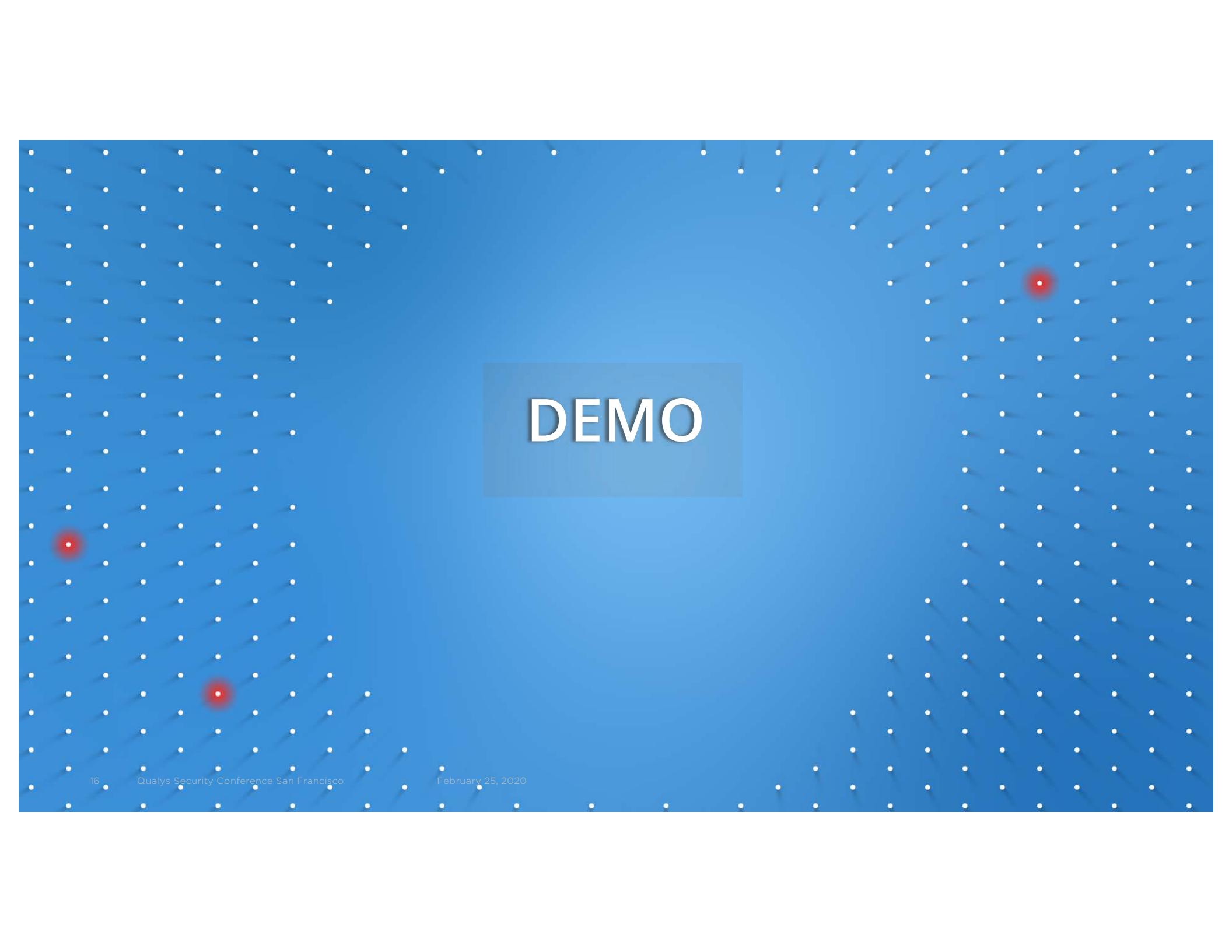
Integrated into Qualys Platform

Function level firewall for containers

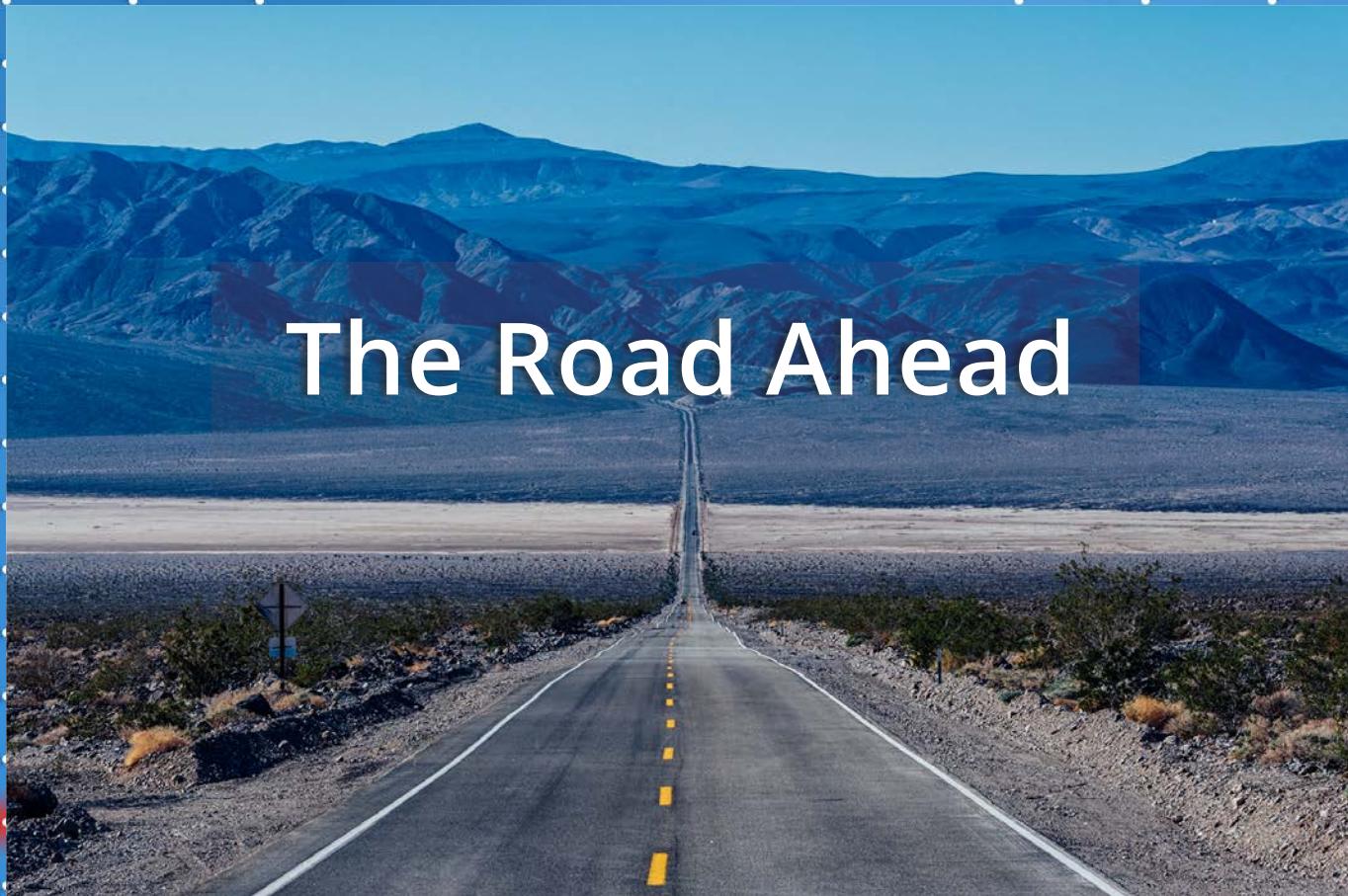
Granular security policies to control file, network, process behavior

Built-in policies from Qualys Threat Research



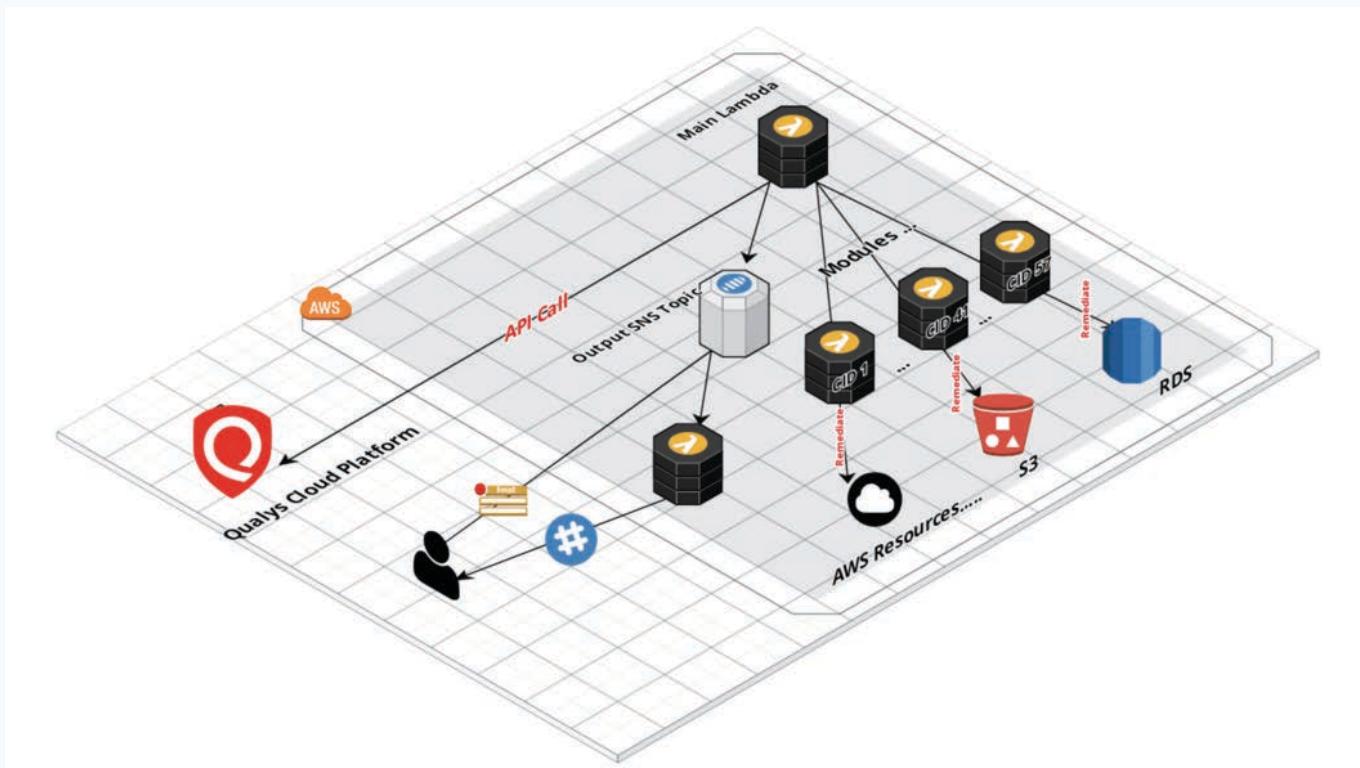


DEMO



The Road Ahead

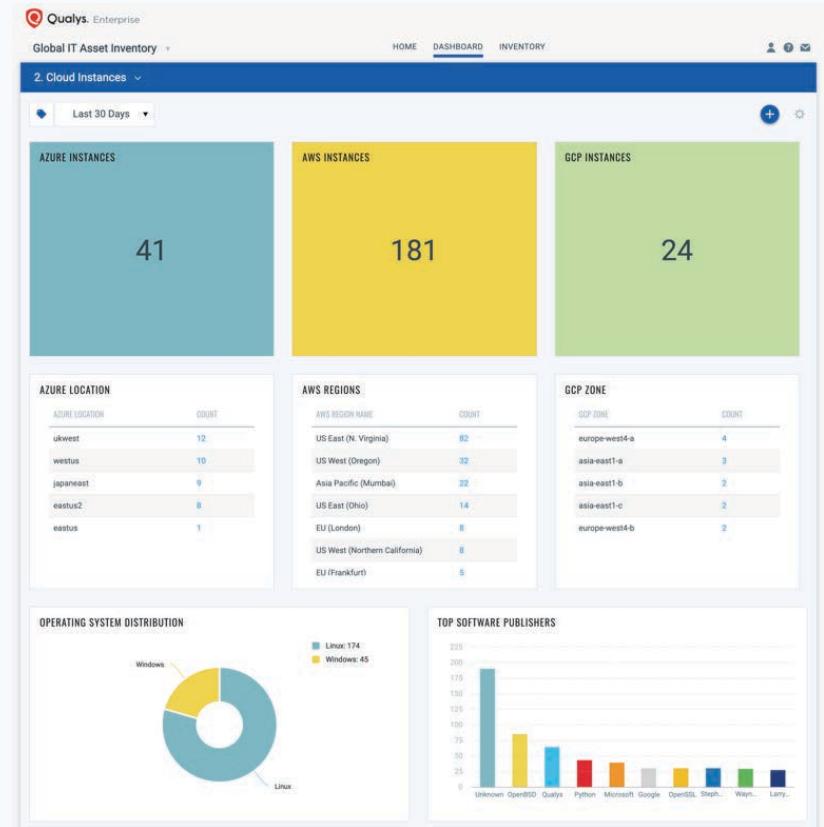
Towards Automated Remediation



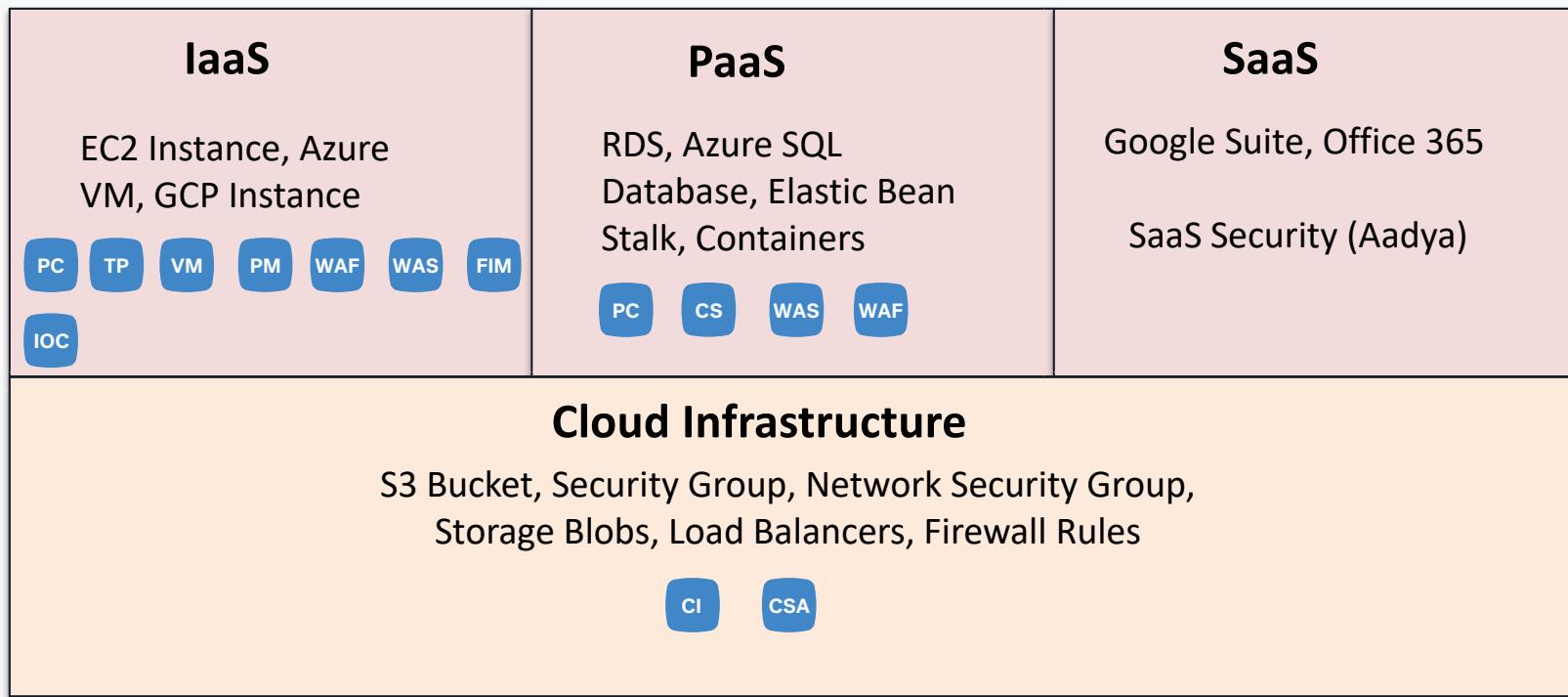
Towards Seamless Visibility

Across application stack (Hosts, Kubernetes Pods, Containers, Serverless)

Correlate cloud inventory data with containers



Securing Your Cloud Deployments





QUALYS SECURITY CONFERENCE 2020

Thank You

Badri Raghunathan
braghunathan@qualys.com